SURVEY ON CAPTCHA-A NEW WAY OF GRAPHICAL SECURITY

Priyanka Sajjan[1] , Prof.Santosh S.Dewar[2]

[1] M.Tech(CSE),Student of BLDEA's Dr.P.G.Halakatti College of Engineering & Technology
Bijapur, Karnataka, (India)

[2] Assistant Professor, Dept.of CSE , BLDEA's Dr.P.G.Halakatti College of Engineering Technology
Bijapur, Karnataka (India)

ABSTRACT

Graphical password schemes have been proposed as an alternative to text based password authentication, because users have difficulty in remembering passwords over time if they choose a secure password i.e. a password that is long and random therefore ,they tend to choose short and insecure passwords which consist of clicking on images rather than typing alphanumeric strings, may help to overcome the problem of creating secure and memorable passwords. In this paper we present a new security primitive based on hard AI problems, namely a novel family of graphical password systems built on top of captcha technology, which we call captcha as a graphical passwords(CGP).CGP addresses several security problems such as online guessing attacks, relay attacks and shoulder surfing attacks.

Keywords: CGP, Captcha, Graphical Password, Hotspots, Passpoints

I. INTRODUCTION

The most common user authentication scheme in computer systems today is the alphanumeric password. Although alphanumeric passwords are used widely, they have certain well known drawbacks such as low memorability of high entropy passwords. These drawbacks are not due to the authentication system itself but arise from the interaction between the users and the system. Since users usually cannot remember high entropy passwords they tend to select short or simple passwords, that can be broken by dictionary attacks. In order to improve the security of user authentication,we use hard AI (Artificial Intelligence), is an exciting new paradigm.Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge.

CGP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CGP are Captcha challenges, and a new CGP image is generated for every login attempt.

CGP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. This threat is widespread and considered as a top cyber security risk [11]. Defence against online dictionary attacks is a more subtle problem than it might appear. CGP requires solving a Captcha challenge in every login.This impact on usability can be mitigated by adapting the CGP image's difficulty level based on the login history of the account and the machine used to log in.

II. LITERATURE SURVEY

Robert Biddle et.al,in their paper "Graphical Passwords:Learning from the First Twelve Years" ,presented a great many graphical password schemes as alternatives to text-based password authentication. In the beginning around 1999, a multitude of graphical password schemes have been proposed,graphical password improved the password memorability and thus usability, while at the same time improving strength against guessing attacks. Text passwords involve alphanumeric and/or special keyboard char- acters, the idea behind graphical passwords is to leverage human memory for visual information, with the shared secret being related to or composed of images or sketches. Like text passwords, graphical passwords are knowledge-based authentication mechanisms where users enter a shared secret as evidence of their identity. Text passwords are easy and inexpensive to implement but the disadvantage is that, passwords are typically difficult to remember, and are predictable if user-choice is allowed. One method to reduce problems related to text passwords is to use password managers. These typically require that users remember only a master password. They store and send on behalf of the user the appropriate passwords to web sites hosting user accounts. Ideally the latter are generated by the manager itself and are stronger than user-chosen passwords. However, implementations of password managers introduce their own usability issues[2] that can exacerbate security problems, and their centralized architecture introduces a single point of failure and attractive target: attacker access to the master password provides control over all of the user's managed accounts. In this paper they have provided a comprehensive review of the first twelve years of published research on graphical passwords. graphical passwords allows for better understanding of knowledge-based authentication in general by looking at issues such as user choice in password selection, memory interference, and the role of cueing in password memorability.

Alain mayer et.al,in their paper "the design and analysis of graphical passwords", they explored an approach to user authentication that generalizes the notion of a textual password and that, in many cases, improves the security of user authentication over that provided by textual passwords. Graphical passwords, which can be input by the user to any device with a graphical input interface. A graphical password serves the same purpose as a textual password, but can consist, for example, of handwritten designs (drawings), possibly in addition to text. The graphical password is due to Blonder [4],the scheme in which the user is presented with a predetermined image on a visual display and required to select one or more predetermined positions on the displayed image in a particular order to indicate his or her authorization to access the resource.In this paper author's have designed two graphical password schemes and those are considered to be more secure than textual passwords. The first graphical password scheme is based on textual password schemes, by enhancing the input of textual passwords using graphical techniques and the second scheme is called "draw a secret"(DAS), which is purely graphical, the user draws a secret design (the password) on a grid.

Susan Wiedenbeck et.al, in their paper "PassPoints: Design and longitudinal evaluation of a graphical password system", described a new, more flexible, and more secure graphical password system that have been designed and implemented, and also the security properties of the system compared to alphanumeric passwords and some other graphical password systems. In 1996 Blonder has proposed his idea for graphical passwords ,his approach was to let the user click, with a mouse or stylus, on a few chosen regions in an image that appeared on the screen. If the user clicks on correct regions, the user was authenticated, otherwise the user was rejected. Most of the graphical password systems can be classified based on either recognition or cued recall. Recognition In a graphical password system,the user has to be able only to recognize previously seen images, not generate them unaided from memory. Cued recall is an intermediary form of recollection between pure recall and pure recognition an example of cued recall is scanning an image to find previously chosen locations in it.The existing graphical password uses these two schemes.A new graphical password scheme is proposed in this paper namely passpoints.This scheme is flexible because it allows any image to be used, e.g. natural images, paintings, etc. The images could be provided by the system or chosen by the user. By using passpoints Graphical password scheme users were able to create a valid password easily , but they had more difficulty learning their passwords than alphanumeric users, taking more trials and more time to complete the practice.

Sonia Chiasson et.al ,in their paper" Influencing Users Towards Better Passwords: Persuasive Cued Click-Points "focuses on Persuasive Cued Click-Points scheme which is effective in reducing the number of hotspots (areas of the image where users are more likely to select clickpoints) while still maintaining usability.This scheme is based on cued click-points scheme. The primary goal of PCCP was to increase the effective password space by guiding users to select more random passwords.Hotspots are a problem in click-based graphical passwords, leading to a reduced effective password space that facilitates more successful dictionary attacks. They investigated whether password choice could be influenced by persuading users to select more random click-points while still maintaining usability[6,7,8]. Using cued click points as a base system, they added a persuasive feature to encourage users to select more secure passwords, and to make it more difficult to select passwords where all five click-points are hotspots. Specifically, when users created a password, the images were slightly shaded except for a randomly positioned viewport. The viewport is positioned randomly rather than specifically to avoid known hotspots, since such information could be used by attackers to improve guesses and could also lead to the formation of new hotspots. The viewport’s size was intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Users were required to select a click-point within this highlighted viewport and could not click outside of this viewport. If they were unwilling or unable to select a click-point in this region, they could press the “shuffle” button to randomly reposition the viewport. While users were allowed to shuffle as often as they wanted, this significantly slowed the password creation process. The viewport and shuffle buttons only appeared during password creation. During password confirmation and login, the images were displayed normally, without shading or the viewport and users were allowed to click anywhere. PCCP encourages and guides users in selecting more random click-based graphical passwords. A key feature in PCCP is that creating a secure password is the “path-of-least-resistance”, making it likely to be more effective than schemes where behaving securely adds an extra burden on users. The approach has proven effective at reducing the formation of hotspots and avoiding known hotspots, thus increasing the effective password space, while still maintaining usability.

Paul Dunphy et.al ,in their paper "Do Background Images Improve Draw a Secret Graphical Passwords?",they presented Draw a Secret [3] ,it is a representative graphical password scheme,in which a user’s password is a free-form drawing produced on an N × N grid. DAS is alphabet independent and so is accessible to users of all languages. However, recent research suggests that DAS users might tend to pick weak graphical passwords that are vulnerable to the graphical dictionary attack [10]. In this paper, they presented their own solution to this problem, a novel variant of the DAS scheme which we call BDAS (Background Draw-a-Secret). In BDAS, instead of creating a password on a blank canvas overlaid with a grid, a user will first choose a background image to be overlaid by the grid, and then draw their secret as in DAS. We aim to study whether this variant will enhance the original scheme. Specifically, we are interested in exploring whether a background image would encourage users to choose more complicated passwords, which are usually less vulnerable to dictionary and other guess attacks. We are also interested in whether the background image could aid users to remember their passwords. BDAS is more effective than DAS both for user authentication and for key generation.

III. METHODOLOGY

3.1 Cgp: An Overview

In CGP, a new image is generated for every login attempt, even for the same user. CGP uses an alphabet of visual objects (e.g., alphanumerical characters, similar animals) to generate a CGP image, which is also a Captcha challenge. A major difference between CGP images and Captcha images is that all the visual objects in the alphabet should appear in a CGP image to allow a user to input any password but not necessarily in a Captcha image. Many Captcha schemes can be converted to CGP schemes, as described in the next subsection.

CGP schemes are clicked-based graphical passwords. According to the memory tasks in memorizing and entering a password, CGP schemes can be classified into two categories: recognition and a new category, recognition-recall, which requires recognizing an image and using the recognized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall, and retains both the recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space.

3.2 User Authentication With Cgp Schemes

Assume that CGP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS). A typical way to apply CGP schemes in user authentication is as follows. The authentication server *AS* stores a salt *s* and a hash value *H(ρ, s)* for each user ID, where *ρ* is the password of the account and not stored. A CGP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects. Upon receiving a login request, *AS* generates a CGP image, records the locations of the objects in the image, and sends the image to the user to click her password. The coordinates of the clicked points are recorded and sent to *AS* along with the user ID. *AS* maps the received coordinates onto the CGP image, and recovers a sequence of visual object IDs or clickable points of visual objects, *ρ*', that the user clicked on the image.

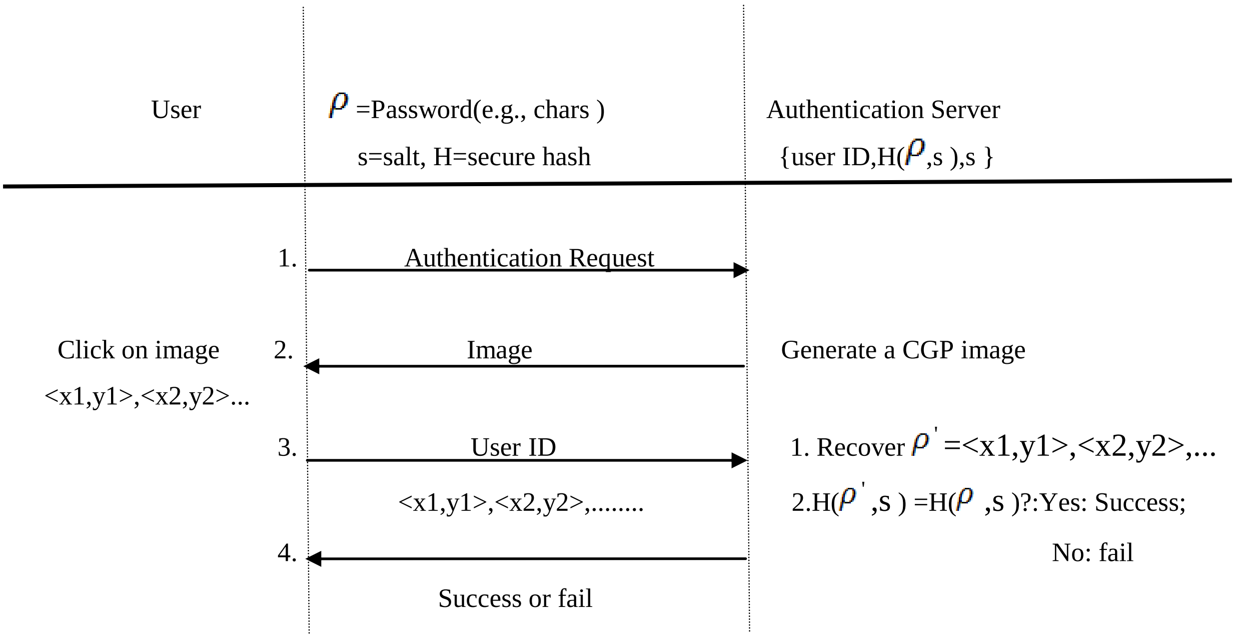

Fig. 1. Flowchart of Basic CGP Authentication

Then *AS* retrieves salt *s* of the account, calculates the hash value of ρ' with the salt, and compares the result with the hash value stored for the account. Authentication succeeds only if the two hash values match. This process is called the basic *CGP* authentication and shown in Fig. 1.

IV. CONCLUSION

We have presented a survey on graphical password scheme that achieve better security than conventional textual passwords.CGP is both captcha and a graphical password scheme. The notion of CGP introduces a new family of graphical passwords ,which adopts a new approach to counter online guessing attacks. a new CGP image, which is also a Captcha challenge, is used for every login attempt to make trials of an online guessing attack computationally independent of each other. CGP forces adversaries to resort to significantly less efficient and much more costly human-based attacks. CGP is also resistant to Captcha relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks and it can also help reduce spam emails sent from a Web email service. Typical application scenarios for CGP include, CGP can be applied on touch-screen devices whereon typing passwords is cumbersome, especially for secure Internet applications such as e-banks. For better results we would need to collect thousands of graphical password data for different types of images. Overall, our work is one step forward in the paradigm of using hard AI problems for security.

REFERENCES

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords:Learning from the first twelve years," ACM Comput. Surveys, vol. 44,no. 4, 2012.

[2] S. Chiasson, P. C.van Oorschot, and R. Biddle."A usability study and critique of two password managers". In 15th USENIX Security Symposium,August 2006.

[3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.

[4] G. Blonder. "Graphical passwords". United States Patent 5559961, 1996.

[5] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction, vol. 1. 2008, pp. 121–130.

[6] Dirik, A.E., Memon, N., and Birget, J.C. Modeling user choice in the PassPoints graphical password scheme. Symp. on Usable Privacy and Security (SOUPS) 2007.

[7] Golofit, K. Click Passwords Under Investigation. ESORICS 2007. LNCS 4734, 343-358, 2007.

[8] Thorpe, J. and van Oorschot, P.C. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. USENIX Security Symp. 2007.

[9] P. Dunphy and J. Yan, "Do background images improve ‘Draw a Secret’ graphical passwords," in Proc. ACM CCS, 2007, pp. 1–12.

[10] J. Thorpe and P. C. van Oorschot. "Graphical Dictionaries and the Memorable Space of Graphical Passwords". Proc. USENIX Security Symposium, 2004.

[11] HP Tipping Point DV Labs, Vienna, Austria. (2010). Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online].Available: http://dvlabs.tippingpoint.com/toprisks2010.